Cisco 700 Series Router Configuration Guide

Software Release 4.4.

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-0184-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

Modifying the equipment without Cisco's written authorization may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

• Turn the television or radio antenna until the interference stops.

• Move the equipment to one side or the other of the television or radio.

• Move the equipment farther away from the television or radio.

• Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Access Registrar, AccessPath, Any to Any, AtmDirector, CCDA, CCDE, CCDP, CCIE, CCNA, CCNP, CCSI, CD-PAC, the Cisco logo, Cisco Certified Internetwork Expert logo, *CiscoLink*, the Cisco Management Connection logo, the Cisco Net*Works* logo, the Cisco Powered Network logo, Cisco Systems Capital, the Cisco Systems Capital logo, Cisco Systems Networking Academy, the Cisco Technologies logo, ConnectWay, ControlStream, Fast Step, FireRunner, GigaStack, IGX, JumpStart, Kernel Proxy, MGX, Natural Network Viewer, NetSonar, Network Registrar, New World, *Packet*, PIX, Point and Click Internetworking, Policy Builder, Precept, RouteStream, Secure Script, ServiceWay, SlideCast, SMARTnet, StreamView, *The Cell*, TrafficDirector, TransPath, ViewRunner, VirtualStream, VisionWay, VlanDirector, Workgroup Director, and Workgroup Stack are trademarks; Changing the Way We Work, Live, Play, and Learn, Empowering the Internet Generation, The Internet Economy, and The New Internet Economy are service marks; and Asist, BPX, Catalyst, Cisco, Cisco IOS, the Cisco IOS logo, Cisco Systems, the Cisco Systems logo, the Cisco Systems Cisco Press logo, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastLink, FastPAD, FastSwitch, IOS, IP/TV, IPX, LightStream, LightSwitch, MICA, NetRanger, Registrar, StrataView Plus, Stratm, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. in the U.S. and certain other countries. All other trademarks mentioned in this document are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any of its resellers. (9906R)

CONTENTS

About This Manual vii

Related Documentation viii

Conventions ix

Chapter 1 Overview 1-1

Supported Protocols 1-1

Software Images 1-2

Administrative Configuration Options 1-3

Chapter 2 Using Profiles with Cisco 700 Series Routers 2-1

Profile Overview 2-1
- Profiles and Connections 2-2

System and Profile Parameters 2-2
- System Mode Parameter Set 2-3
- Profile Mode Parameter Set 2-3
- Permanent Profiles 2-4

Creating and Modifying Profiles 2-5
- Displaying Profile Configurations 2-5
- Removing Profile-Based Values 2-5
- Deleting Profiles 2-6
- Changing Profile Names 2-6

Incoming Calls 2-6

Outgoing Calls 2-7

Chapter 3 Basic Configurations 3-1

Basic Configuration Concepts 3-1
- Bridges and Routers 3-2
- Profiles 3-2
- LANs and WANs 3-2
- Current Configuration 3-3
- Remote and Central Sites 3-4

Password and Secret 3-4
Additional Reference 3-4

Starting Point 3-4
Setting SPID Autodetection (North America only) 3-5
Setting SPIDs Manually (North America only) 3-6

Bridging with a Cisco 700 Series Router 3-7
Cisco 700 Series Router Bridging Instructions 3-8

Routing IP with a Cisco 700 Series Router to an ISP 3-9
Routing a Cisco 700 Series Router to an ISP Instructions 3-11

Routing IP to a Central Site 3-11
Central Site IP Routing Command Summary 3-13

Routing IP and IPX On-Demand 3-14
On-Demand IP and IPX Routing with PPP Instructions 3-16
Central Site On-Demand IP and IPX Routing with PPP Commands 3-17

Chapter 4 Using CHAP 4-1

SPID Detection (North America only) 4-2

IP Static Routing and Callback with CHAP Authentication 4-2
Remote Cisco 765 Command Summary 4-3

IP Static Routing with CHAP Authentication and MLP 4-4
Remote Cisco 765 Command Summary 4-5

IP Static Routing with PAP Authentication and MLP 4-6
Remote Cisco 765 Command Summary 4-7

IP Unnumbered Static Routing and CHAP with MLP 4-8
Remote Cisco 765 Command Summary 4-9

IP Static and IPX Static Routing with CHAP and MLP 4-10
Remote Cisco 765 Command Summary 4-11

IPX Static Routing with CHAP and MLP 4-12
Remote Cisco 765 Command Summary 4-13

Multilink PPP Encapsulation 4-14

Dynamic Routing Protocols 4-14

Bridging to a Router Running Cisco IOS Software 4-15

Chapter 5 Configuring DHCP Relay, DHCP Server, and PAT 5-1

DHCP Description 5-2
DHCP Server Application Notes 5-2
DHCP Relay Application Notes 5-3

PAT Description 5-3
PAT Application Notes 5-3

IPCP Description 5-4
IPCP Address Negotiation Application Notes 5-4

PPP IPCP Negotiation Example 5-5
Cisco 765 Series Router Commands 5-5
Verify the Configuration 5-6

DHCP Relay with IPCP Negotiation Example 5-6
Cisco 765 Series Router Commands 5-6
Verify the Configuration 5-7

DHCP Server with IPCP Negotiation Example 5-7
Cisco 765 Series Router Commands 5-8
Verify the Configuration 5-8

PAT with IPCP Single-Destination Negotiation Example 5-9
Cisco 765 Series Router Commands 5-10
Verify the Configuration 5-10

DHCP Server and PAT with IPCP Single-Destination Negotiation Example 5-11
Cisco 765 Series Router Commands 5-12
Verify the Configuration 5-12

DHCP Server with PAT and IPCP Dual-Destination PPP Negotiation Example 5-13
Cisco 765 Series Router Commands 5-14
Verify the Configuration 5-15

Chapter 6 Configuring Remote CAPI 6-1

CAPI and RVS-COM 6-2
Supported D-Channel Protocols 6-3
Supported Applications 6-3
Remote CAPI Router Commands 6-3

Configuring the Cisco 700 Router as an RCAPI Server 6-4
RCAPI Command Summary 6-4
Verify the Configuration 6-5

Appendix A Token Card and Cisco Secure Authentication Support A-1

Token Caching A-2

About This Manual

This chapter discusses the organization, related documentation, and conventions of the *Cisco 700 Series Router Configuration Guide*.

This document is organized as follows:

- Chapter 1, “Overview,” provides a brief overview of Cisco IOS-700 software and supported protocols.
- Chapter 2, “Using Profiles with Cisco 700 Series Routers,” describes a set of user-defined parameters grouped in a customized profile and associated with a specific remote device.
- Chapter 3, “Basic Configurations,” describes how to connect a Cisco 700 series router to an Internet service provider (ISP) or to a central site, such as your company network.
- Chapter 4, “Using CHAP,” describes how to connect a Cisco 700 series router to a router running Cisco IOS software.
- Chapter 5, “Configuring DHCP Relay, DHCP Server, and PAT,” describes how to configure Dynamic Host Configuration Protocol (DHCP) relay, DHCP server, and Port Address Translation (PAT) on the Cisco 700 series router.
- Chapter 6, “Configuring Remote CAPI,” describes how to configure Remote Common Application Programmers Interface (CAPI) and the ISDN Device Control Protocol (ISDN-DCP) on the Cisco 700 series router.
- Appendix A, “Token Card and Cisco Secure Authentication Support,” describes the Token Card and Cisco Secure Authentication Support security features.

Related Documentation

The following documentation is also provided with your Cisco 700 series router:

- *Release Notes for Cisco 700 Series Router Software* provides the latest information on the router software. Release notes for previous versions of the software are on the Cisco Documentation CD-ROM and the Cisco Web site.
- *Cisco 760 Quick Reference Guide and Cisco 770 Quick Reference Guide* provide hardware installation instructions and forms to assist you in gathering configuration information. Each guide includes a Cisco 700 Fast Step CD-ROM.
- *Cisco 700 Series Router Command Reference* provides details of all router commands. The document is available on the Cisco Documentation CD-ROM and the Cisco Web site in HTML format.
- *Cisco 700 Series Router Installation Guide* provides instructions for cabling the Cisco 700 series router. The document is available on the Cisco Documentation CD-ROM and the Cisco Web site in HTML format. A paper copy of the document is provided with your router.

Additional Cisco documentation and literature are available in a CD-ROM package that ships with your Cisco 700 series router. The Documentation CD-ROM, a member of the Cisco Connection family, is updated monthly. Therefore, it may be more up to date than the printed documentation. To order additional copies of the Documentation CD-ROM, contact your local sales representative or call customer service. You can also access Cisco documentation on the World Wide Web at http://www.cisco.com, http://www-china.cisco.com, or http://www-europe.cisco.com.

Cisco 700 series router configuration information can be found at http://www.cisco.com/warp/public/779/smbiz/service/configs/700_configs.htm and http://www.cisco.com/warp/cpropub/67/sample.html

If you are reading Cisco product documentation on the World Wide Web, you can submit comments electronically. Click **Feedback** in the toolbar, and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco. We appreciate your comments.

Conventions

This publication uses the following conventions to convey instructions and information:

- The caret character (^) represents the Control key.

  For example, the key combinations ^D and Ctrl-D are equivalent: Both mean hold down the Control key while you press the D key. Keys are indicated in capitals, but are not case sensitive.

- A string is defined as a nonquoted set of characters.

  There are a few strings that include quotation marks as part of the statement. Therefore, common practice is not to include the quotation marks unless they are included in the statement. For example, *set the SNMP community string to public* does not use quotation marks around the string “public” because when you enter the string, you would not include the quotation marks.

Command descriptions use these conventions:

- Vertical bars (|) separate alternative, mutually exclusive, elements.
- Square brackets ([ ]) indicate optional elements.
- Variables for which you supply values are in *italic*.
- Examples that contain system prompts denote interactive sessions, indicating the user enters the command at the prompt. The system prompt indicates the current command mode. For example, the prompt router:2503> indicates profile mode. The exception is when a list of commands is provided in an example configuration; the prompt is not shown for the sake of clarity.
- Fixed information you enter is in **`boldface`** `screen` font. Variable information you enter is in *italic*.
- Terminal sessions and information the system displays are in `screen` font.
- Nonprinting characters, such as passwords, are in angle brackets (< >).

The command syntax contains a combination of bold and regular uppercase and lowercase alphanumeric characters. You can enter the full text of the commands, or you can enter the abbreviated form. The abbreviated form consists of the first characters in each word, shown in uppercase bold in the command syntax. The uppercase bold characters are the minimum you must enter for the command to be recognized and executed.

The actual commands you enter are not case sensitive. The capitalization and bold type are used in this manual only to differentiate the characters required for the abbreviated forms of commands.

For example, The syntax of the **set system** command is as follows:

SEt **SY**stemname [*systemname*]

The complete version of the **set system** command can be entered at the command prompt as follows:

```
>set systemname systemname
systemname>
```

The abbreviated version of the same command can be entered as follows:

```
>se sy systemname
systemname>
```

Note Means *reader take note*. Notes contain helpful suggestions or references to materials not contained in this manual.

Timesaver This symbol means the described action *saves time*. You can save time by performing the action described in the paragraph.

Caution This symbol means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

CHAPTER 1

Overview

Cisco 700 series routers connect small office Ethernet LANs to corporate networks through Integrated Services Digital Network (ISDN) Basic Rate Interface (BRI) lines. After configuration, the router automatically routes packets to and from remote destinations using IP or Internetwork Packet Exchange (IPX).

The Cisco 700 series router is a *fixed configuration* router. The router operating system is called Cisco IOS-700 software and is unique to the Cisco 700 series router.

Supported Protocols

The Cisco 700 series routers support the following protocols:

- IP
- IPX
- Internet Protocol Control Protocol (IPCP)
- Internet Control Message Protocol (ICMP)
- Internetwork Packet Exchange Control Protocol (IPXCP)
- Point-to-Point Protocol (PPP)
- Bridge Control Protocol (BCP)
- Multilink PPP (MLPPP)
- Address Resolution Protocol (ARP)
- Service Advertisement Protocol (SAP)
- Password Authentication Protocol (PAP)

- Trivial File Transfer Protocol (TFTP server)
- Simple Network Management Protocol (SNMP)
- Routing Information Protocol (RIP) for IP and IPX
- Triggered RIP for IP
- Challenge Handshake Authentication Protocol (CHAP)
- Dynamic Host Configuration Protocol (DHCP)
- Port Address Translation (PAT)
- Remote Common Application Programmers Interface (RCAPI)
- ISDN Device Control Protocol (ISDN-DCP)

Software Images

The Cisco 700 Series routers run a proprietary Cisco software (Cisco IOS-700 software) image, which is different than traditional Cisco IOS software. The image you use varies, depending on the region in which the router is used and what feature set you desire. The image name, for example, c760-in.r-TPH.43-1.bin, designates the region and features. The regions are as follows:

- US for use in North America
- NET3 for use in Europe
- TR6 for use in Germany
- INS for use in Japan
- TPH for use in Australia

The features are indicated as follows:

- Internet Ready (IP only, 30 users with data compression on) images have a "b" designation.
- Internet Ready X.25 (IP only, 30 LAN devices, compression, X.25) images have a "bxd" designation.

- Remote Office (IP/IPX, 1500 LAN devices, compression) images have an "r" designation.
- Remote Office X.25 (IP/IPX, 1500 LAN devices, compression, X.25) images have an "rxd" designation.

So the example image named "c760-in.b-TPH.43-1.bin" is a Series 760 router image software Release 4.3(1) with the Internet Ready feature set for Australia. (All Cisco 700 series routers run Series 760 router images. There are no Series 770 router images.)

You can verify the image loaded on your router by entering the **version** command at the command-line prompt. The following example shows a router running a Cisco 760 (c760) image for the United States (US), release 4.0(1), and using the Remote Office (r) feature set:

```
guest> version
Software Version c760-in.r.US 4.0(1) - Jan 14 1997 19:00:23
Cisco 766
ISDN Stack Revision US 2.10 (5ESS/DMS/NI-1)
```

Administrative Configuration Options

You can configure routers through the configuration port or across an IP network using Telnet. In addition, Cisco IOS-700 software supports Cisco 700 Fast Step software applications. These tools are on the Cisco 700 Fast Step CD-ROM in the *Cisco 700 Quick Reference Guide*.

CHAPTER 2

Using Profiles with Cisco 700 Series Routers

A profile is a set of configuration parameters associated with ports on the router or WAN devices.

This chapter contains the following sections:

- Profile Overview
- System and Profile Parameters
- Creating and Modifying Profiles
- Incoming Calls
- Outgoing Calls

Profile Overview

There are two modes in which you can set parameters, the system mode and the profile mode. System mode parameters affect the configuration on a global level. Profiles are sets of local parameters. Profile mode parameters affect how the router handles the connection to a device.

You do not have to reconfigure the router every time you connect to a different device. Instead of using one set of configuration parameters for all devices, you can use different profiles to communicate with a variety of devices.

For example, you can create a user-defined profile called 2500 that contains the parameters to be used when communicating with a Cisco 2500 series router over the WAN. You can customize your Cisco 700 series router to maintain up to 17 user-defined profiles. Profiles are saved in the Cisco 700 series router nonvolatile RAM (NVRAM).

In addition to user-defined profiles, there are three permanent profiles, Internal, LAN, and Standard. The Internal profile stores parameters used to communicate between the LAN and WAN ports on the Cisco 700 series router. The LAN profile stores parameters that configure the LAN port on the router. The Standard profile is the default profile. If authentication is not required and the destination device you are connecting to does not have a user-defined profile, the router uses the Standard profile.

Profiles and Connections

Profiles are either active or inactive. An active profile creates a *virtual connection* to the remote device associated with the profile. A virtual connection is a connection without physical channels. After creating a virtual connection, an on-demand call can be made to the associated remote device to establish a *physical connection*.

A physical connection is a dynamically created pipeline of packets from the Cisco 700 series router to a switch on the WAN. All connections are associated with the profile that defines the configuration of the connection.

Virtual and physical connections behave similarly; the difference is that physical connections forward packets to the WAN. Virtual connections monitor packet traffic on the LAN until a demand filter “sees” that a packet is destined for the WAN and initiates a call to the switch, opening the physical connection. Once the call is established, the virtual connection becomes an active physical connection, and the packets move through the pipeline.

System and Profile Parameters

The system is composed of both system mode parameters, user-defined profiles, and permanent profiles. System mode parameters can be changed only in system mode. The prompt indicates you are in system mode by displaying nothing or the router name. An example of the prompt is shown below:

```
Router_name>
```

If you are in profile mode, the profile name appears on the prompt, separated from the system name by a colon (:). An example of the prompt is shown below:

```
Router_name:Profile>
```

All profiles are based on the profile template and inherit the system-level values. When you create a new profile, its default values are taken from the profile template.

System Mode Parameter Set

System mode parameters affect the router as a system. Table 2-1 lists the system parameters.

Table 2-1 System Parameter Set

Caller ID parameters	Call waiting	PPP[1] parameters
Date and time	Country group	Screen length
Directory number(s)	Address age time	Screen echo
Delay time	Local and remote access	SNMP[2] parameters
Forwarding mode	Phone 1 and 2	SPIDs[3]
Multidestination dialing	PPP client password	Switch type
Numbering plan	PPP client secret	System password
Patterns	Voice priority	Power Source 1 detect
Passthru	Compression	System name
PPP authentication		

1 PPP = Point-to-Point Protocol
2 SNMP = Simple Network Management Protocol
3 SPID = service profile identifier

Profile Mode Parameter Set

Changes made to profile mode parameters in system mode affect the profile template. When a profile is created, it inherits the matching system mode parameters from the profile template. Any changes to parameters in profile mode apply only to that profile. Changes made to profile parameters in system mode are stored in the profile template. When you use the **set user** command to create a user-defined profile, the default parameters for the new profile are taken from system mode.

Table 2-2 lists the parameters that can be configured in a profile.

Table 2-2 Profile Parameters

Bridging	Line speed	PPP authentication (outgoing)
Ringback number	Auto calling	All IP parameters, including filters
Passthrough	Demand	PAP password (client and host)
Learning	Timeout	All IPX parameters, including filters
Subnet mask	Called number	CHAP secret (client and host)
Protocol	Encapsulation	Bridge filters (address, type, and user-defined)
Loopback		

Permanent Profiles

Cisco 700 series routers contain three permanent profiles. Permanent profiles can be modified, but they cannot be deleted. The permanent profiles are as follows:

LAN — Determines how data is passed from the router to the LAN. This profile is commonly used for connections made directly to the local network.

Internal — Determines how data is passed between the bridge engine and the IP/IPX router.

Standard — The default profile. If authentication is set to none and a profile does not exist for the WAN switch, the router uses the Standard profile by default. If authentication is required and no profile is found, the call is dropped.

The decision to use the LAN or Internal profile involves some knowledge of your network design and whether you are bridging or routing to remote sites (or a combination of both). It is best to use the LAN profile instead of the Internal profile to simplify the configuration. You can easily associate the LAN profile with the Ethernet interface and the user-defined profiles with the ISDN interface.

Sometimes situations arise (very infrequent) where you must route a protocol to one site and bridge the *same* protocol to another site. Simply leave the LAN profile as a bridging profile, and use the Internal profile for all routed protocol information.

Creating and Modifying Profiles

A new profile is created with the **set user** command. When you create a new profile, you automatically enter profile mode for that profile. The following example creates a user profile called tomd. Enter the **set user** command to create a profile using the profile template for the default values of the parameters, as follows:

```
Host> set user tomd
Host:tomd>
```

Notice that the profile mode is indicated by the prompt, which appears as the system name *and* the profile name, separated by a colon. While this prompt is displayed, modifications to the parameters only affect the parameters in the profile. The changes do not affect system mode parameters or other profiles.

The **cd** command is used to change to system mode or to another profile. Following is an example of the **cd** command used to change to a permanent profile called LAN:

```
Router_name> cd LAN
Router_name:LAN>
```

Note that the prompt includes the name of the profile. You can now modify the LAN profile parameters.

Displaying Profile Configurations

The **show** commands display the values associated with a profile parameter in profile mode. The commands work in system mode to show the values associated with parameters in the profile template.

In profile mode, some **show** commands only display profile parameters. Parameter values that have been redefined in profile mode are indicated with a <*>. All other parameter values are inherited from the profile template.

Removing Profile-Based Values

You can remove any parameter value within a profile with the **unset** command. The parameter you removed inherits its value from the system mode.

In the following example, the profile parameter number is removed from the profile by using the **unset** command:

```
Host:Profile> unset number
```

Deleting Profiles

The **reset user** command deletes a user-defined profile from the router. The three permanent profiles (LAN, Internal, and Standard) cannot be deleted. This command also closes any connection associated with the profile.

In the following example, the tomd profile is removed from the system by using the **reset user** command:

```
Host:Profile> reset user tomd
```

Changing Profile Names

The **set profile user** command changes the name of an existing profile. Enter this command while in profile mode for the profile you want to affect. In the following example, the profile name is being changed from 2500 to 4500:

```
766:2500> set profile user 4500
766:4500>
```

Incoming Calls

When the router receives an incoming call, the router searches both active and inactive profiles for a profile with the same name as the calling device. If it finds a profile with the matching user ID, the router uses the configuration parameters of that profile while communicating with the remote device. If the profile is inactive, it is automatically activated for the duration of the connection.

When the call is finished, the physical link between the two devices is disconnected. However, the virtual connection to the remote router might be configured to remain active.

If the profile is configured to remain active after a link disconnects, a virtual connection remains. The virtual connection monitors the LAN traffic. If packets destined for the WAN are detected, the router opens up the physical connection and forwards the packets.

If the profile is configured to become inactive after a link disconnects, both the physical link and the virtual connection to the remote router are disconnected until another call is received from the same remote router.

Outgoing Calls

Outgoing calls require that the associated user-defined profiles be set to active, that the **set auto** command be on, and that a phone number to call be stored in the profile. If the profile is inactive, a number to dial is not available to the router.

CHAPTER 3

Basic Configurations

This chapter contains basic configuration examples for connecting a Cisco 700 series router to an Internet service provider (ISP) or to a central site, such as your company network. It is assumed that your router is cabled as described in the *Cisco 700 Quick Reference Guide*. Before you proceed with the examples in this chapter, have the information regarding ordering the ISDN line and the connection information in the *Cisco 700 Quick Reference Guide* (shipped with your router package) available.

The chapter is written so that a knowledgeable beginner can perform a basic configuration of the router, guided by the examples. Explanations are kept to a minimum, but they do show how the individual commands fit into the framework of a configuration.

This chapter has the following sections:

- Basic Configuration Concepts
- Starting Point
- Setting SPIDs Manually (North America only)
- Bridging with a Cisco 700 Series Router
- Routing IP with a Cisco 700 Series Router to an ISP
- Routing IP to a Central Site
- Routing IP and IPX On-Demand

Basic Configuration Concepts

The information in this section describes basic networking concepts as they relate to the Cisco 700 series router and the examples presented. If you have some experience with Cisco 700 series routers, you can skip this section.

Bridges and Routers

Routers forward packets on to specific network segments based on a logical network address, reducing network traffic by keeping unnecessary packets off network segments by only forwarding packets to segments as required.

A bridge joins individual network segments into a single network. The bridge floods packets on to all the network segments it is connected to. In other words, bridges offer simplicity and routers offer a greater degree of control. Cisco 700 series routers can function as a bridge and a router.

Profiles

Profiles are logically organized sets of commands for each connection that can be customized and stored independently. This allows you to configure your router for more than one connection. There are two types of profiles, *permanent* and *user-defined*. The *Cisco 700 Series Router Command Reference* publication contains an extensive discussion on profiles. It is important to understand the use of profiles before attempting to configure your router.

LANs and WANs

Cisco 700 series routers have a "LAN side" and a "WAN side." The LAN side of the router is the Ethernet 10BaseT connection where your computer (or another short-range network device) is connected to the router. The WAN side is ISDN. The configuration commands can affect function on one or both sides of the router. Which side is affected depends upon the command and the profile containing the command.

Current Configuration

You can display the current configuration at any time using the **show configuration** command. If you issued the command in system mode, system mode commands display. If you issue the command in profile mode, profile mode commands display. An asterisk (*) next to a value indicates the value has been modified from the default value. The command is entered as follows:

```
>show config
```

The following sample display shows output for the Cisco 700 series routers, from the **show configuration** command in system mode:

```
Host> show config
System Parameters
    Environment
      Screen Length          20
      Echo Mode              ON
      CountryGroup           1
    Bridging Parameters
      LAN Forward Mode       ANY
      WAN Forward Mode       ONLY
      Address Age Time       OFF
    Call Startup Parameters
      Multidestination       OFF
    Line Parameters
      Switch Type            5ESS
    Call Parameters          Link 1             Link 2
      Retry Delay              30                 30

Profile Parameters
    Bridging Parameters
      Bridging               ON
      Routed Protocols
      Learn Mode             ON
      Passthru               OFF
    Call Startup Parameters
      Encapsulation          PPP
    Line Parameters
      Line Speed             AUTO
      Numbering Plan         NORMAL
    Call Parameters          Link 1             Link 2
      Auto                     ON                 ON
      Called Number
      Ringback Number
```

Remote and Central Sites

In the examples, the Cisco 700 series router you are configuring is referred to as the *remote* router. This is strictly for identification purposes and does not have anything to do with geography or the physical location of the router.

Password and Secret

There are several types of authentication, such as Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP). To avoid confusion, the PAP password is referred to as *password*, and the CHAP secret password is referred to as *secret*. The PAP password is plain text. The CHAP secret is encrypted.

Additional Reference

For more information on the commands, basics of networking, profiles and so forth, refer to the *Cisco 700 Series Router Command Reference* publication. The *Cisco 700 Series Command Reference* publication also contains advanced configuration examples.

Starting Point

This section shows how to set the router to default values and provide basic configuration information used in all configurations. All of the example configurations assume default values unless otherwise indicated.

Step 1 Use the **set default** command as follows to be sure that you begin with all default values when configuring your router:

```
> set def
```

System-level parameters and the parameters in the permanent profiles are set to their default values. Existing user-defined profiles are deleted and the router reboots.

Step 2 Enter the **set directorynumber** command (usually a ten-digit local number with no spaces or dashes) to set the ISDN directory numbers.

```
>set 1 directory number 4085551234
>set 2 directory number 4085551235
```

You are ready to set Service Profile Identifier (SPID) automatic detection. A SPID is a number provided by the ISDN carrier to identify the line configuration of the BRI service. Each SPID points to line setup and configuration information.

Setting a SPID is described in the section “Setting SPID Autodetection (North America only)” in this chapter (recommended if you are connecting to a service provider where the ISDN switch type is DMS-100 or National ISDN-1 (NI1)) or to enter the SPIDs manually, as described in the section “Setting SPIDs Manually (North America only)” in this chapter.

Setting SPID Autodetection (North America only)

If the service provider ISDN switch type is DMS-100 or National ISDN-1 (NI1), the router supports an automatic SPID detection feature. This section describes how to set the autodetection feature. If the switch type is 5ESS Custom PPP, do not enter SPIDs; go to the next section.

Enable automatic SPID detection feature as follows:

```
>set autodetection on
```

Once you enable the autodetection feature, wait for the router to complete the process. This process might take several minutes to complete. When autodetection is successful, the following messages display:

```
>L76   1             Auto Spid Detect Successful 5ESS
>L76   1  055512340  Auto Spid Detect Successful
>L76   2  055512350  Auto Spid Detect Successful
```

No additional procedures are required. You can now enter specific configuration information.

If autodetection fails, the following message displays:

```
>L84  Manually enter spids and set autodetection off
```

In this event, set autodetection off by using the **set autodetection** command and continue with the section “Setting SPIDs Manually (North America only)” to enter SPIDs manually.

Setting SPIDs Manually (North America only)

SPIDs can be detected automatically using the **set autodetection** command, or SPIDs can be entered manually, as described in this section.

If the service provider switch type is 5ESS Custom PPP, you do not need to enter SPIDs; go to the next section. If the service provider switch type is DMS-100, National (NI1), or 5ESS Multipoint, continue with this section.

To enter the SPIDs assigned by your ISDN service provider, take the following steps:

Step 1 Enter the **set switch** command to configure the ISDN switch type that is being used with your ISDN line:

```
> set switch dms
```

Step 2 Enter the **set spid** command to set the router's SPID numbers:

```
> set 1 spid 0510198765430
> set 2 spid 0510187654320
```

You are ready to configure the router for a specific routing environment.

An AT&T 5ESS switch can support up to eight SPIDs per BRI line. Because multiple SPIDs can be applied to a single B channel, multiple services can be supported simultaneously. For example, the first B channel can be configured for data, and the second B channel can be configured for both voice and data. In this scenario, the second B channel can support an ISDN telephone in addition to supporting data connections. For 5ESS switches, the SPID is usually the 10-digit ISDN number beginning with "01" and ending with "0." For example: ISDN number, 4085551212; SPID, 0140855512120. (There is no standard format for SPIDs. As a result, SPID values can vary, depending on the switch vendor and the carrier.)

DMS-100 and NI1 switches support only two SPIDs, with only one B channel per SPID. If both B channels will be used for data only, enter the two SPIDs (one for each B channel). An issue comes up when trying to run data and voice over the same B channel. Assuming the first SPID is applied to the first B channel for data traffic and is limited to that B channel only, this leaves only one other SPID for the second B channel.

Consequently, the second B channel can be used for either data or voice, but not both simultaneously. The absence or presence of the second SPID in the configuration dictates whether the second B channel can be used for data or voice. This is an example of SPID

values for DMS-100 and NI1 switches: ISDN number, 4085551212; SPID 1, 408555121201; SPID 2, 408555121202. In this case the SPID is the 10-digit ISDN number ending with a “01” for SPID 1 and a “02” for SPID 2.

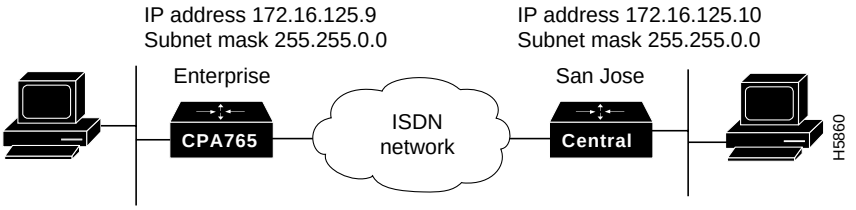
Bridging with a Cisco 700 Series Router

This section describes how to bridge a Cisco 700 series router over an ISDN line to another router. Bridging is used in cases where you do not need a lot of filtering to manage the network. Basically, you are relying on the nodes on the LAN side of the router to determine if a packet should be accepted or dropped. (If you turn routing on, you can filter the packets on the WAN side, reducing your traffic on the LAN side.)

Note Bridging over an ISDN line is not an efficient use of ISDN bandwidth. Routing over the ISDN line helps optimize ISDN bandwidth by reducing traffic to the WAN.

Figure 3-1 illustrates an example of a remote Cisco 700 series router bridging to a router called *central* at a central site.

Figure 3-1 Bridging Example



You are going to establish a basic connection with another router, relying primarily on the defaults. In this example configuration, a simple user-defined profile is created in your Cisco 700 series router to bridge over an ISDN network to another router.

By default, the Cisco 700 series router automatically “learns” the MAC addresses that exist locally and remotely across the WAN. The router stores the MAC addresses in a MAC address table, so it knows if the unicast packets should remain on the LAN or forwarded

across the ISDN line. In a bridging scenario, the router does not need an IP address and bridging occurs regardless. The IP address is used when the router is being managed remotely by a Telnet session or participating in SNMP.

Both sides of the WAN must be configured with PPP host names, secrets, and passwords for authentication. Each profile must also include dialing information.

Cisco 700 Series Router Bridging Instructions

The IP address and subnet mask are not entered. IP address assignments are not necessary in a bridged network; they are used only if the router is being pinged or accessed through Telnet or SNMP.

Following is the command summary for configuring the Cisco 700 series router to bridge to the router called *central* at the central site:

```
set system CPA765
set user central
set active
set ppp secret client
set ppp password client
set bridging on
set 1 number phone_number
set 2 number phone_number
reboot
```

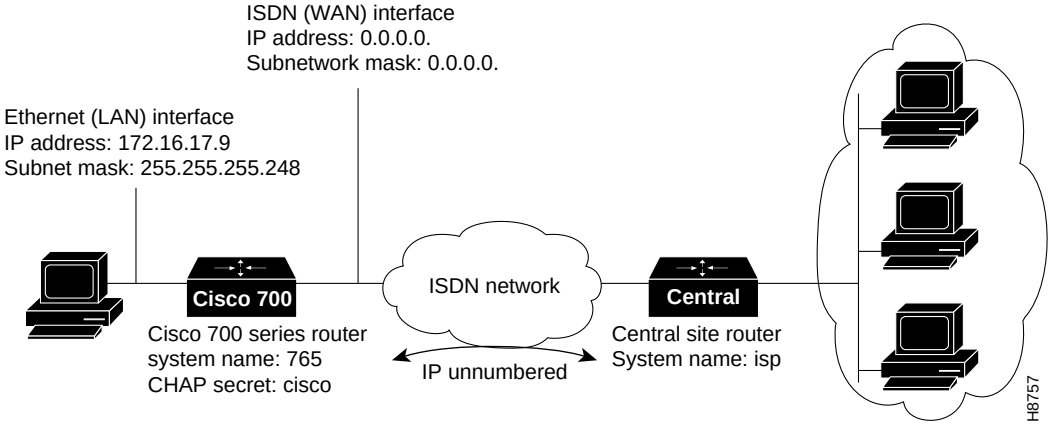
Routing IP with a Cisco 700 Series Router to an ISP

This section describes how to configure a Cisco 700 series router to route to an ISP by using Internet Protocol (IP). Figure 3-2 illustrates the configuration used in this example. By default, PPP incoming authentication is on and outgoing authentication is off.

Note If you are connecting to an Ascend device, you must disable PPP Bandwidth Allocation Control Protocol (BACP) and PPP multilink.

The example also uses an unnumbered IP address on the Cisco 700 series router and a dynamically-assigned IP address from the ISP, a common practice used to conserve IP addresses.

Figure 3-2 Connecting to an ISP–Example Configuration



In this example, a user-defined profile named *isp* is created, representing the ISP router. Your router uses the *isp* profile to initiate the call to the ISP router.

When the Cisco 700 series router calls the ISP router, it sends the ISP the PPP host name, the CHAP secrets, and PAP passwords, depending upon what the other router requires to authenticate the call.

Routing a Cisco 700 Series Router to an ISP Instructions

Following is the command summary for configuring the remote Cisco 700 series router to connect to an ISP:

```
set system 764
cd lan
set ip address 172.16.17.9
set ip netmask 255.255.255.248
set ip routing on
set user isp
set number 5558011
set ppp password client
set ppp secret client
set ppp address negotiation local on
set ip routing on
set ip route destination 0.0.0.0/0 gateway 0.0.0.0 propagate on
set bridging off
set ip address 0.0.0.0
set ip netmask 0.0.0.0
set timeout 360
set ip pat on
set active
reboot
```

If you are being charged for each connection, you can use the **set timeout** command to set the timeout to zero. Doing so maintains your connection and minimizes the number of fees.

Routing IP to a Central Site

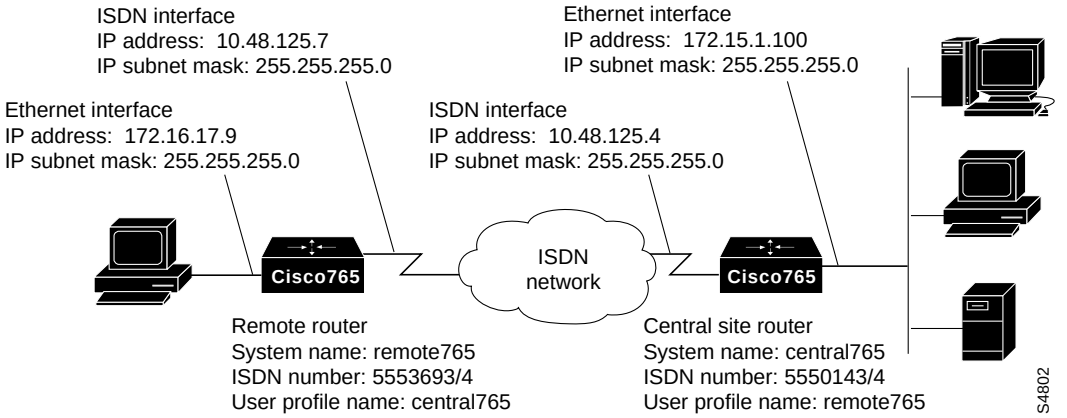
This section describes how to configure a remote Cisco 765 router and a central site Cisco 765 router for on-demand IP routing using PPP.

PPP addresses issues that include the assignment and management of IP addresses, asynchronous (start/stop) and bit-oriented synchronous encapsulation, network protocol multiplexing, error detection, and option negotiation.

PPP addresses these issues by providing an extensible Link Control Protocol (LCP) and a family of Network Control Protocols (NCPs) to negotiate optional configuration parameters and facilities. PPP supports IP and IPX.

Figure 3-3 is an illustration of the configuration used in this example.

Figure 3-3 Routing IP to a Central Site—Example Configuration



In this example, the Cisco 765 router named *remote765* is used to establish a connection through the ISDN service provider to the corporate network at a central site.

Central Site IP Routing Command Summary

Following is the command summary for configuring the remote Cisco 765 router for on-demand IP routing using PPP:

```
set system remote765
set multidestination on
cd LAN
set ip address 172.16.17.9
set ip netmask 255.255.255.0
set ip routing on
set ip rip update periodic
set user central765
set ppp password client
set ppp secret client
set ip address 10.48.125.7
set ip netmask 255.255.255.0
set ip routing on
set ip rip update demand
set ip route destination 0.0.0.0/0 gateway 10.48.125.4
set number 5550143
set timeout 360
set active
reboot
```

Following is the command summary for configuring the central site Cisco 700 series router for on-demand IP routing with PPP:

```
set system central766
set multidest on
set ppp auth in chap
set ppp secret host
cd lan
set ip address 172.15.1.100
set ip netmask 255.255.255.0
set ip routing on
set ip rip update periodic
set user remote765
set ppp auth out chap
set ppp secret client
set bridging off
set ip address 10.48.125.4
set ip netmask 255.255.255.0
set ip routing on
set ip rip update demand
set ip route destination 0.0.0.0 gateway 10.48.125.7
set ip rip version 1
set 1 number 5553693
set 2 number 5553694
set timeout 360
set active
reboot
```

The **set ip rip update demand** command is only applicable to the Cisco 700 series router.

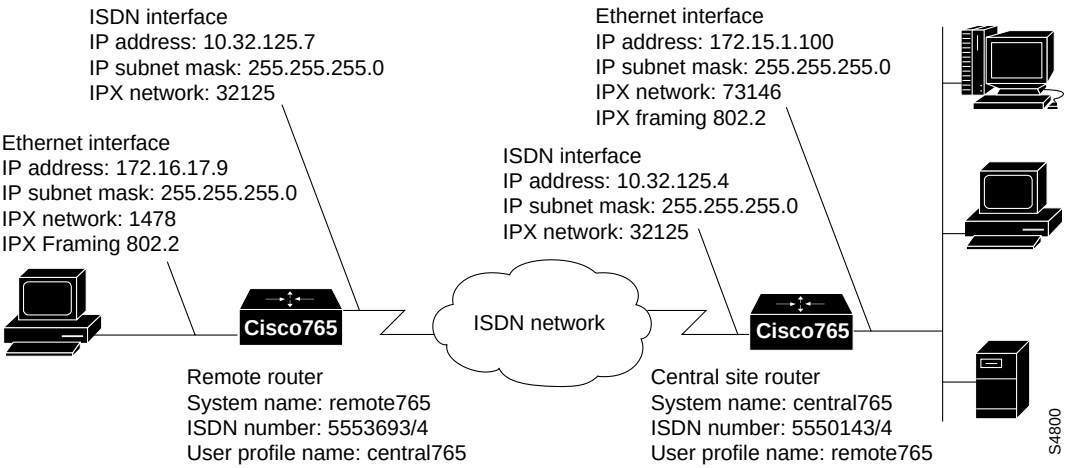
If you are being charged for each connection, you can use the **set timeout** command to set the timeout to zero. Doing so maintains your connection and minimizes the number of fees.

Routing IP and IPX On-Demand

This section describes how to configure the remote Cisco 765 router and the central site Cisco 765 router for on-demand IP and IPX routing using PPP.

Figure 3-4 illustrates the configuration used in this example.

Figure 3-4 Routing IP and IPX On-Demand—Example Configuration



The remote Cisco 765 router is used to establish a connection through the ISDN service provider to the corporate network at a central site using PPP. The remote Cisco 765 router has three permanent profiles: LAN, Internal, and Standard. This example uses the LAN profile and a user-defined profile.

On-Demand IP and IPX Routing with PPP Instructions

Following is the command summary for configuring the remote Cisco 765 router for on-demand IP and IPX routing using PPP:

```
set system remote765
set multidestination on
set ppp password client
set ppp secret client
set ppp auth out chap
set ppp password host
set ppp secret host
cd LAN
set ipx routing on
set ipx network 1478
set ipx framing 802.2
set ipx rip update periodic
set ip address 172.16.17.9
set ip netmask 255.255.255.0
set ip routing on
set ip rip update periodic
set user central765
set ipx routing on
set ipx network 32125
set ipx rip update demand
set ipx spoof 10
set ip route destination 0.0.0.0/0 gateway 10.32.125.4
set ip address 10.32.125.7
set ip netmask 255.255.255.0
set ip routing on
set ip rip update demand
set 1 number 5550143
set 2 number 5551044
set timeout 360
set active
reboot
```

Central Site On-Demand IP and IPX Routing with PPP Commands

Following is the command summary for configuring the central site Cisco 700 series router router for on-demand IP and IPX routing using PPP:

```
set system central765
set multidestination on
set ppp auth in chap
set ppp secret client
cd lan
set ipx routing on
set ipx network 73146
set ipx framing 802.2
set ipx rip update periodic
set ip address 172.15.1.100
set ip netmask 255.255.255.0
set ip routing on
set ip rip update periodic
set user remote765
set bridging off
set 1 number 5553693
set 2 number 5553694
set ipx network 32125
set ipx routing on
set ipx framing none
set ipx rip update demand
set ipx spoof 10
set ip route destination 0.0.0.0/0 gateway 10.32.125.7
set ip address 10.32.125.4
set ip netmask 255.255.255.0
set ip routing on
set ip rip update demand
set ppp auth out chap
set ppp secret host
reboot
```

CHAPTER 4

Using CHAP

This chapter contains configuration examples for connecting a Cisco 700 series router to a router running Cisco IOS software. In these examples, the remote router is a Cisco 765 series router, and the central site router is a Cisco 4500 series router. Any Cisco 700 series router can be used in place of the remote Cisco 765 series router. Any router running Cisco IOS software can replace the central site Cisco 4500 series router.

In these examples, the Cisco 4500 series router serial-interface configuration is an ISDN Primary Rate Interface (PRI). Depending on the router model used at the central site, the serial interface might be a different type.

In addition, this chapter lists several interoperability issues that exist between Cisco IOS software and Cisco 700 series routers. These issues must be considered if you are connecting your Cisco 700 series router to a router running Cisco IOS software.

This chapter contains the following sections:

- IP Static Routing and Callback with CHAP Authentication
- IP Static Routing with CHAP Authentication and MLP
- IP Static Routing with PAP Authentication and MLP
- IP Unnumbered Static Routing and CHAP with MLP
- IP Static and IPX Static Routing with CHAP and MLP
- IPX Static Routing with CHAP and MLP
- Multilink PPP Encapsulation
- Dynamic Routing Protocols
- Bridging to a Router Running Cisco IOS Software

SPID Detection (North America only)

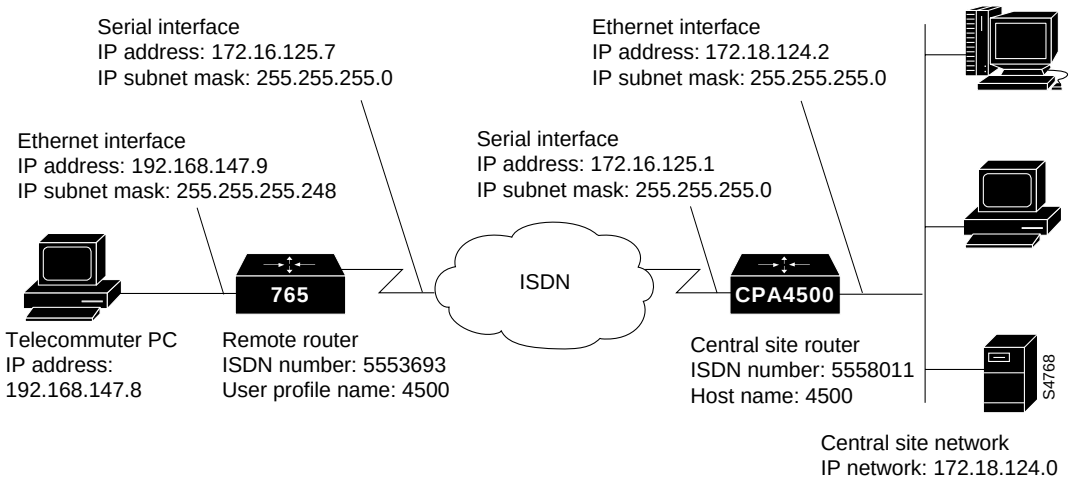
In North America, SPIDs can be automatically detected or manually configured. For more information on SPID detection, see "Setting SPID Autodetection (North America only)" and "Setting SPIDs Manually (North America only)" in the "Basic Configurations" chapter.

IP Static Routing and Callback with CHAP Authentication

This section describes how to configure the routers for Internet Protocol (IP) static routing and callback with Challenge Handshake Authentication Protocol (CHAP).

Figure 4-1 illustrates the configuration used in this example.

Figure 4-1 IP Static Routing and Callback with CHAP Authentication



Remote Cisco 765 Command Summary

Following is the command summary for configuring the remote Cisco 765 series router for IP static routing and callback with CHAP authentication:

```
set switch 5ess
set 1 dir directory_number
set 2 dir directory_number
set system 765
set ppp authentication incoming chap
set ppp secret client
set multidestination on
cd lan
set ip address 192.168.147.9
set ip netmask 255.255.255.248
set ip routing on
set ip rip update periodic
set ip rip receive v2
set ip rip version 2
set user 4500
set ppp secret client
set ppp secret host
set ip route destination 0.0.0.0 gateway 172.16.125.1 propagate on
set ip address 172.16.125.7
set ip netmask 255.255.255.0
set ip routing on
set ip framing none
set ppp callback request always
set 1 ringback number
set 2 ringback number
set number 5558011
set bridging off
set ip rip update off
set timeout 360
set active
reboot
```

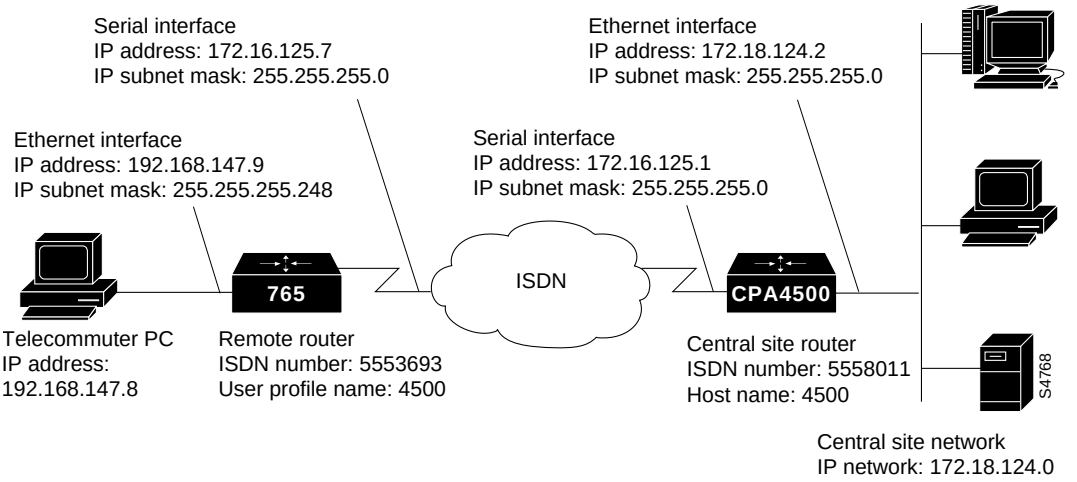
Multilink PPP is enabled by default. If the Cisco 700 series router is dialing into a host that does not support multilink PPP or that does not have multilink PPP enabled, the Cisco 700 series router might report a misconfiguration. This is most commonly seen when the Cisco 700 series router is connected to equipment from Ascend.

IP Static Routing with CHAP Authentication and MLP

This section describes how to configure the central site Cisco 4500 series router and the remote Cisco 765 series router for IP static routing with Challenge Handshake Authentication Protocol (CHAP) and Multilink Protocol (MLP).

Figure 4-2 is an illustration of the configuration used in this example.

Figure 4-2 IP Static Routing with CHAP Authentication and MLP



Remote Cisco 765 Command Summary

Following is the command summary to configure the remote Cisco 765 series router for IP static routing with CHAP and MLP:

```
set switch 5ess
set 1 dir directory_number
set 2 dir directory_number
set system 765
set multidestination on
set ppp multilink on
set ppp authentication incoming chap
set ppp authentication outgoing chap
cd lan
set ip address 192.168.147.9
set ip netmask 255.255.255.248
set ip routing on
set ip rip update periodic
set user 4500
set ppp secret client
set ip address 172.16.125.7
set ip netmask 255.255.255.0
set ip routing on
set ip framing none
set ip route destination 0.0.0.0 gateway 172.16.125.1 propagate on
set number 5558011
set bridging off
set ip rip update off
set ppp secret host
set timeout 360
demand 2 threshold 32 duration 5
set active
reboot
```

Note The **set ppp authentication outgoing chap** command in this example is not recommended when connecting to Ascend 4000 or NAS routers.

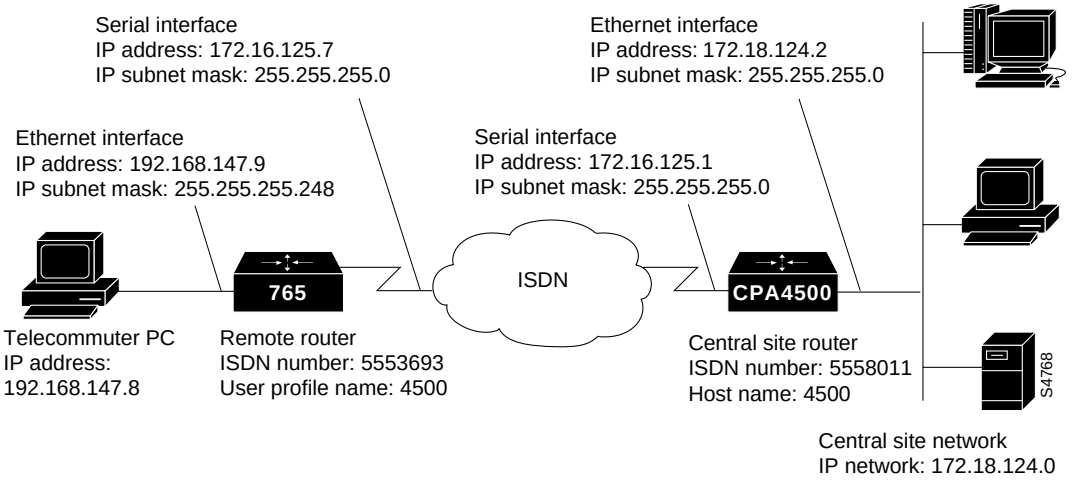
For detailed information regarding the commands listed here, refer to the *Cisco 700 Series Router Command Reference*.

IP Static Routing with PAP Authentication and MLP

This section describes how to configure the central site Cisco 4500 series router and the remote Cisco 765 series router for Internet Protocol (IP) static routing with Password Authentication Protocol (PAP) authentication.

Figure 4-3 is an illustration of the configuration used in this example.

Figure 4-3 IP Static Routing with PAP Authentication



Remote Cisco 765 Command Summary

Following is the command summary to configure the remote Cisco 765 series router for IP static routing with PAP authentication:

```
set switch 5ess
set 1 dir directory_number
set 2 dir directory_number
set system 765
set multidestination on
set ppp multi on
set ppp authentication in pap
set ppp authentication out pap
cd lan
set ip address 192.168.147.9
set ip netmask 255.255.255.248
set ip routing on
set ip rip update periodic
set ip rip receive v2
set ip rip version 2
set user 4500
set ip route destination 0.0.0.0 gateway 172.16.125.1 propagate on
set ip address 172.16.125.7
set ip netmask 255.255.255.0
set ip routing on
set ip framing none
set ppp clientname 765
set ppp password client
set ppp password host
set number 5558011
set bridging off
set timeout 360
set active
reboot
```

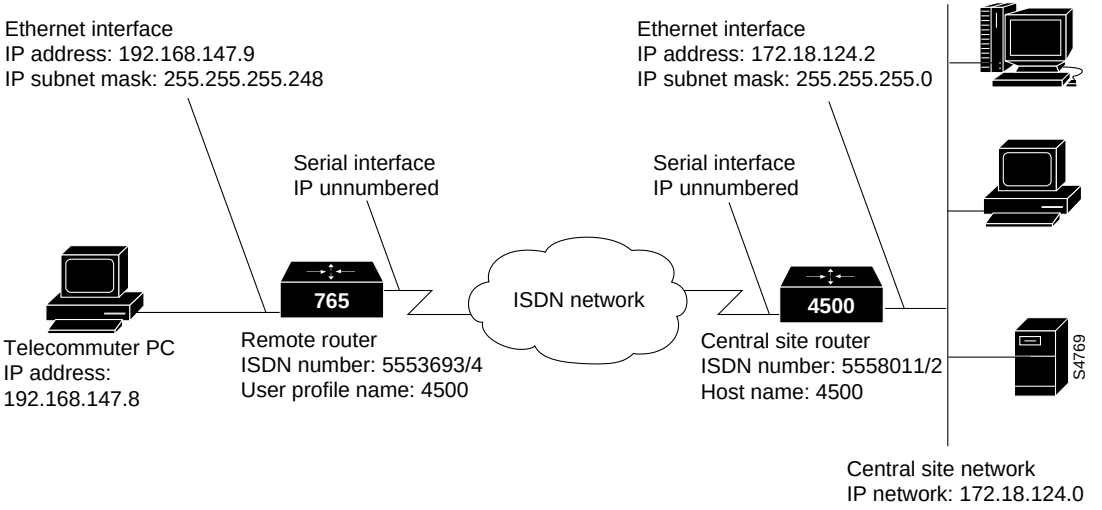
For detailed information regarding the commands listed here, refer to the *Cisco 700 Series Router Command Reference*.

IP Unnumbered Static Routing and CHAP with MLP

This section describes how to configure the central site Cisco 4500 series router and the remote Cisco 765 series router for Internet Protocol (IP) unnumbered routing with Challenge Handshake Authentication Protocol (CHAP) authentication and Multilink Protocol (MLP).

Figure 4-4 is an illustration of the configuration used in this example.

Figure 4-4 IP Unnumbered Routing and CHAP Authentication with MLP



Remote Cisco 765 Command Summary

Following is the command summary for configuring the remote Cisco 765 series router for IP unnumbered routing with CHAP authentication and MLP:

```
set switch 5ess
set system 765
set multidestination on
set ppp multilink on
set ppp authentication incoming chap
set ppp authentication outgoing chap
set ppp secret client
set ppp secret host
cd lan
set ip address 192.168.147.9
set ip netmask 255.255.255.248
set ip routing on
set ip rip update periodic
set ip rip receive v2
set ip rip version 2
set user 4500
set ppp secret client
set ip rip update off
set ip routing on
set ip framing none
set ip route destination 0.0.0.0 gateway 0.0.0.0
set number 5558011
set bridging off
set ppp secret host
set timeout 360
set active
reboot
```

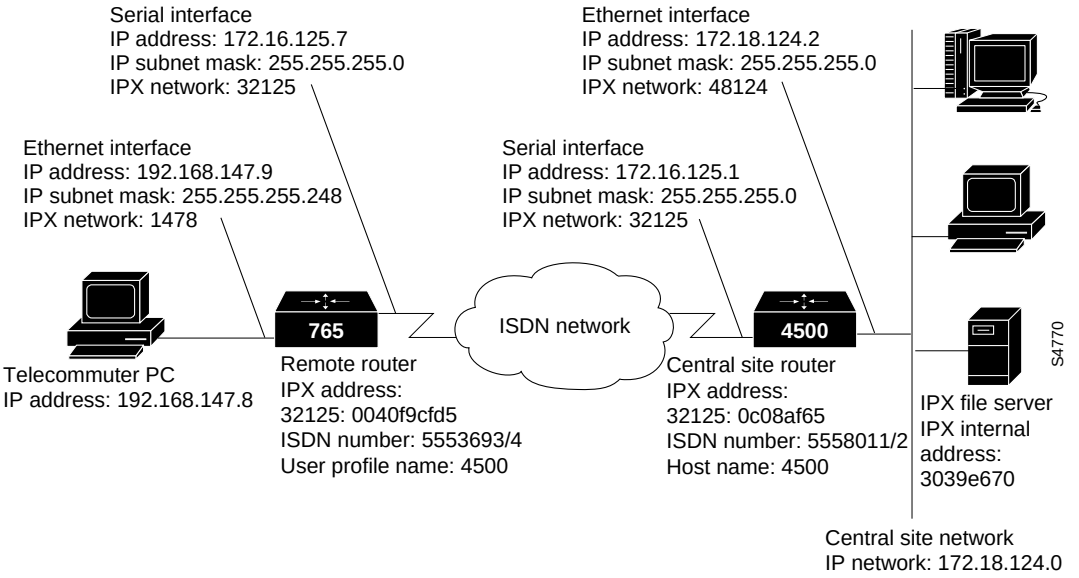
For detailed information regarding the commands listed here, refer to the*Cisco 700 Series Router Command Reference.*

IP Static and IPX Static Routing with CHAP and MLP

This section describes how to configure the central site Cisco 4500 series router and Cisco 765 series router for Internet Protocol (IP) static and Internetwork Packet Exchange (IPX) static routing with Point-to-Point Protocol (PPP) using CHAP and MLP.

Figure 4-5 is an illustration of the configuration used in this example.

Figure 4-5 IP Static and IPX Static Routing with PPP



Remote Cisco 765 Command Summary

Following is the command summary to configure the remote Cisco 765 series router for IP static and IPX static routing with PPP using CHAP and MLP:

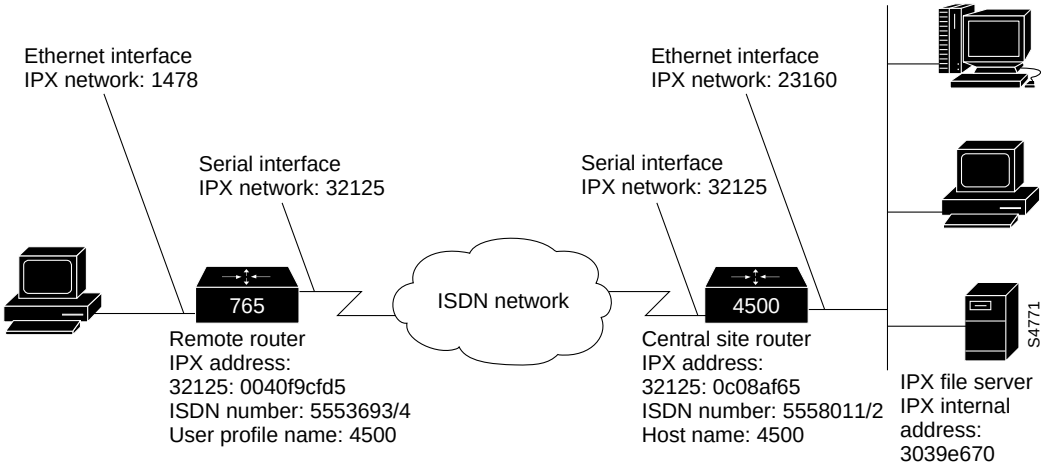
```
set switch 5ess
set 1 dir directory_number
set 2 dir directory_number
set system 765
set multidestination on
set ppp authentication incoming chap
set ppp authentication outgoing chap
set ppp secret client
set ppp secret host
cd lan
set ipx network 1478
set ipx framing 802.2
set ipx routing on
set ipx rip update periodic
set ip address 192.168.147.9
set ip netmask 255.255.255.248
set ip routing on
set ip rip update periodic
set user 4500
set ipx network 32125
set ipx routing on
set ipx route destination 3039e670 gateway 32125:0c08af65
set ipx service name CORP_FS1 type 4 address 3039e670:01:0451
set ipx spoof 10
set ipx rip update off
set ipx framing none
set ip routing on
set ip route destination 0.0.0.0 gateway 172.16.125.1 propagate on
set ip address 172.16.125.7
set ip netmask 255.255.255.0
set ip framing none
set number 5558011
set bridging off
set ip rip update off
set timeout 360
set active
reboot
```

IPX Static Routing with CHAP and MLP

This section describes how to configure the remote Cisco 765 series router and the central site Cisco 4500 series router for Internetwork Packet Exchange (IPX) static routing with Point-to-Point Protocol (PPP).

Figure 4-6 is an illustration of the configuration used in this example.

Figure 4-6 IPX Static Routing with PPP



Remote Cisco 765 Command Summary

Following is the command summary for configuring the remote Cisco 765 series router for IPX static routing with PPP:

```
set switch 5ess
set 1 dir directory_number
set 2 dir directory_number
set system 765
set multidestination on
set ppp auth in chap
set ppp secret client
set ppp secret host
set multilink on
cd lan
set ipx network 1478
set ipx framing 802.2
set ipx routing on
set ipx rip update periodic
set user 4500
set ppp secret client
set ipx network 32125
set ipx routing on
set ipx route destination 3039e670 gateway 32125:0c08af65
set ipx service name CORP_FS1 type 4 address 3039e670:01:0451
set ipx spoofing 10
set ipx rip update off
set ipx framing none
set number 5558011
set bridging off
set timeout 360
set active
reboot
```

For detailed information regarding the commands listed here, refer to the*Cisco 700 Series Router Command Reference*.

Multilink PPP Encapsulation

Cisco 700 series routers implement multilink PPP, which is available in Release 11.0(3) or later of Cisco IOS software. You can disable multilink PPP in the following two environments:

- You are connecting your Cisco 700 series router to a router running a Cisco IOS release prior to 11.0(3).
- You are connecting your Cisco 700 series router to a router running Cisco IOS Release 11.0(3) or later, *and* you have not configured multilink PPP on that router running Cisco IOS.

Use the **set ppp multilink** command at the system level to disable multilink PPP, as follows:

```
766> set ppp multilink off
```

Dynamic Routing Protocols

Cisco 700 series routers implement RIP Versions 1 and 2 and demand RIP. Demand RIP is not implemented in Cisco IOS software. If you are connecting your router to a router running Cisco IOS software, and you want to use a dynamic routing protocol, you must disable demand RIP.

Use one of the following **set ip rip update** commands to disable demand RIP:

```
766> set ip rip update periodic / snapshot
```

or

```
766> set ip rip update none
```

Note Setting the IP RIP update to **periodic** maintains the connection indefinitely. This might be a concern if it is not necessary to maintain the line 24 hours a day, 7 days a week; you are paying for connection time that you are not using.

Bridging to a Router Running Cisco IOS Software

It is possible to bridge data over ISDN to and from Cisco ISDN routers. Depending on your network environment, this might be an ideal solution. Bridging offers configuration simplicity with few concerns regarding network address space limitations and unroutable protocols. Bridging also offers compatibility with other products that need to bridge.

When bridging, you do not have the same ISDN line control that routing access lists provide. When bridging protocols such as Novell IPX, AppleTalk, or NetBIOS, it is possible for the ISDN line to remain connected for long periods of time. This can result in high ISDN usage charges. If bridging is the only solution for your environment, we recommend monitoring the ISDN line connection.

Cisco IOS Release 11.1 and earlier limit the number of simultaneous ISDN bridge sessions to one per interface.

Prior to Cisco IOS Release 11.2 (half-bridging), the Cisco IOS must also be configured to the bridging protocol, not the router protocol.

CHAPTER 5

Configuring DHCP Relay, DHCP Server, and PAT

Cisco 700 series routers can perform the role of the relay agent, relaying IP configuration information request packets from the LAN interface, over the ISDN interface, to a specified Dynamic Host Configuration Protocol (DHCP) server. Cisco 700 series routers provide DHCP relay, DHCP server, Port Address Translation (PAT), and Internet Protocol Control Protocol (IPCP).

This chapter provides descriptions, application notes, and example configurations for configuring Dynamic Host Configuration Protocol (DHCP) relay, DHCP server, and Port Address Translation (PAT) on the Cisco 700 series router. It contains the following sections:

- DHCP Description
- PAT Description
- IPCP Description
- PPP IPCP Negotiation Example
- DHCP Relay with IPCP Negotiation Example
- DHCP Server with IPCP Negotiation Example
- PAT with IPCP Single-Destination Negotiation Example
- DHCP Server and PAT with IPCP Single-Destination Negotiation Example
- DHCP Server with PAT and IPCP Dual-Destination PPP Negotiation Example

DHCP Description

DHCP is a client-server protocol that allows devices on an IP network (the DHCP clients) to request configuration information from a DHCP server. DHCP allocates network addresses from a central pool on an as-needed basis. DHCP is useful for assigning IP addresses to hosts connected to the network temporarily or for sharing a limited pool of IP addresses among a group of hosts that do not need permanent IP addresses.

DHCP allows for increased automation and fewer network administration problems by:

- Eliminating the need for the manual configuration of individual computers, printers, and shared file systems.
- Preventing the simultaneous use of the same IP address by two clients.
- Allowing configuration from a central site.

DHCP Server Application Notes

The following are application notes for DHCP server:

- DHCP relay and DHCP server are mutually exclusive.
- When DHCP server is initialized, default addresses are used if no LAN or internal address exists. The Cisco 700 series router picks up the DHCP client's default gateway, netmask, and starting DHCP addresses by using the LAN IP address, if one exists. If a LAN address does not exist, the router uses the internal IP address. If neither exists, it uses the default settings: 10.0.0.1 as the LAN IP address (default gateway for DHCP clients), 255.0.0.0 as the subnet mask, and 10.0.0.2 as the starting DHCP client addresses.
- For the DHCP values to be automatically generated based on the LAN or internal IP address, each DHCP value must be set to **0.0.0.0** or **none**, for the new values to take effect.

DHCP Relay Application Notes

The following are application notes for DHCP relay:

- The IP address in the Internal profile must be on the same network as that of the DHCP clients.
- A firewall configuration (where there is an Internal profile and LAN IP address) does not work with DHCP relay.
- A configuration where PAT is on and DHCP relay is enabled is not valid. DHCP relay will attempt to cross from a public to a private domain. PAT prevents access to the private domain. DHCP relay fails because it must reference the router's private address.
- DHCP relay and DHCP server are mutually exclusive. The Cisco 700 series router can function as one or the other, but not both.

PAT Description

Cisco 700 series routers provide PAT, enabling local hosts on a private IP network to communicate externally.

Packets destined for an external address have their private IP address plus port number translated to the router's external IP address before the IP packet is forwarded to the WAN. IP packets returning to the router have their external IP addresses (plus port number) translated back to the private IP addresses, and the packets are forwarded to the LAN.

When PAT is enabled, the transmission of RIP packets is automatically disabled to prevent a broadcast of the private IP addresses externally.

PAT Application Notes

A configuration where PAT is on and DHCP relay is enabled is not valid. DHCP relay will attempt to cross from a public to a private domain. PAT prevents access to the private domain. DHCP relay fails because it must reference the router's private address.

IPCP Description

If you are using IP routing, Cisco 700 series routers must be configured for IPCP to connect to routers running Cisco IOS software. Use the **set ip framing** command in profile mode to enable IPCP for user-defined WAN profiles by setting IP framing to **none**.

The following example illustrates IPCP enabled by disabling IP framing:

```
766:2503> set ip framing none
```

Note Do not set the **ip framing** or the **ipx framing** commands to **none** when configuring the permanent LAN profile.

IPCP Address Negotiation Application Notes

The following are application notes for IPCP address negotiation:

- Cisco 700 series routers require a user-defined profile, configured with IP routing on, to receive an IPCP addresses.
- A router running Cisco IOS software must be configured to hand off IPCP addresses.
- If a manually configured IP address exists on the Internal profile of a Cisco 700 series router, the IPCP address is assigned to the WAN profile.
- If a manually configured IP address exists on the LAN profile, the IPCP address is assigned to the Internal profile.

PPP IPCP Negotiation Example

This section describes how to configure a remote Cisco 700 series router for PPP IPCP negotiation to a central site router, such as a Cisco 4500 series router, that is running Cisco IOS software.

Figure 5-1 is an illustration of the configuration used in this example.

Figure 5-1 PPP IPCP Negotiation

Cisco 765 Series Router Commands

Following are the commands for configuring the remote Cisco 765 series router for point-to-point IPCP negotiation with a Cisco 4500 router:

```
set switch 5ess
set 1 dir directory_number
set 2 dir directory_number
set system 765
set user 4500
set ppp secret client
set ppp password client
set active
set 1 number phone_number
set 2 number phone_number
set ip routing on
set ip route destination 0.0.0.0/0 gateway 0.0.0.0
set ip rip version 2
set ip rip receive v2
set ip rip update linkup
reboot
```

For detailed information regarding the commands listed here, refer to the *Cisco 700 Series Router Command Reference.*

Verify the Configuration

You can use the **show ip configuration all** and **show ip route all** commands to see the IPCP negotiation address.

DHCP Relay with IPCP Negotiation Example

This section describes how to configure a remote Cisco 700 series router for DHCP relay with IPCP negotiation to a central-site router running Cisco IOS software.

Figure 5-2 is an illustration of the configuration used in this example.

Figure 5-2 DHCP Relay with IPCP Negotiation

Cisco 765 Series Router Commands

Following are the commands for configuring the remote Cisco 765 series router for DHCP Relay with IPCP Negotiation with a Cisco 4500 router:

```
set system 765
set dhcp relay 172.168.100.2
set user 4500
set 1 number phone_number
set 2 number phone_number
set ip routing on
set ip rip version 2
set ip rip receive v2
set ip rip update linkup
reboot
```

For detailed information regarding the commands listed here, refer to the *Cisco 700 Series Router Command Reference.*

Verify the Configuration

You can use the **show ip configuration** and **show ip route** commands to see the IPCP negotiation address.

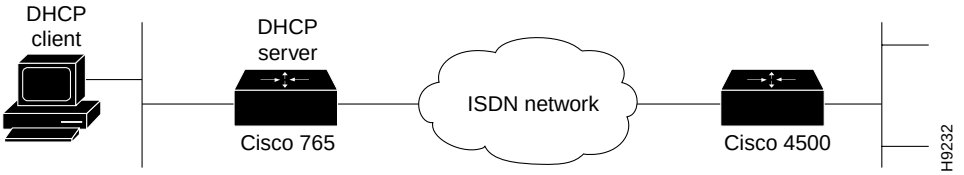
You can use the **show dhcp configuration** command to see the IP address returned by DHCP.

DHCP Server with IPCP Negotiation Example

This section describes how to configure a remote Cisco 700 series router as a DHCP server with IPCP negotiation to a central-site router running Cisco IOS software.

Figure 5-3 is an illustration of the configuration used in this example.

Figure 5-3 DHCP Server with IPCP Negotiation



Cisco 765 Series Router Commands

Following are the commands for configuring the remote Cisco 765 series router as a DHCP server with IPCP negotiation with a Cisco 4500 router:

```
set switch NI-1
set 1 dir 5551211
set 2 dir 5551212
set 1 spid 88855512110101
set 2 spid 88855512120101
set system 765
set dhcp server
set dhcp address 172.168.1.2 128
set dhcp netmask 255.255.255.0
set dhcp gateway primary 172.168.1.1
cd lan
set ip address 172.168.1.1
set ip netmask 255.255.255.0
set ip routing on
set user 4500
set ip routing on
set active
set 1 number phone_number
set 2 number phone_number
set ip routing on
set ip rip version 2
set ip rip receive v2
set ppp address negotiation local on
set ip rip update periodic
reboot
```

For detailed information regarding the commands listed here, refer to the *Cisco 700 Series Router Command Reference.*

Verify the Configuration

When a call is made, you can use the **show ip configuration all** and **show ip route all** commands to see the IPCP negotiation address.

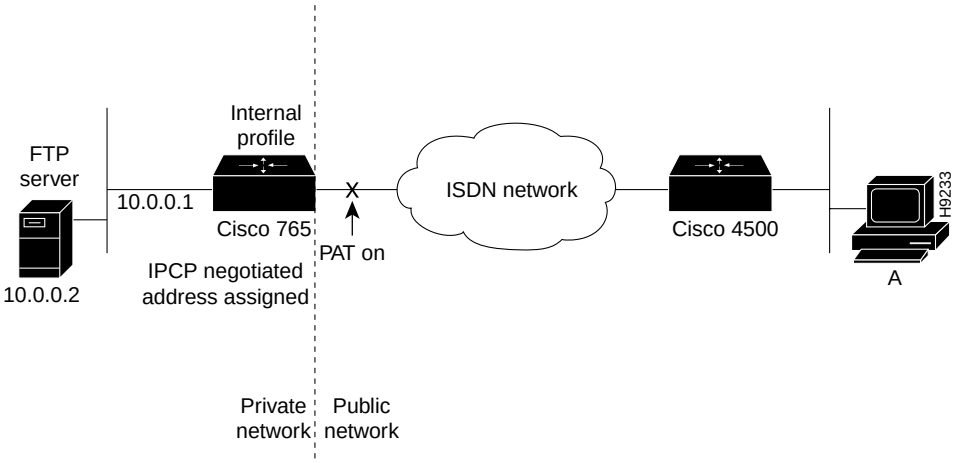
You can use the **show dhcp configuration** command to see the IP address returned by DHCP.

PAT with IPCP Single-Destination Negotiation Example

This section describes how to configure a remote Cisco 700 series router for PAT with IPCP single-destination negotiation to a central-site router running Cisco IOS software.

Figure 5-4 is an illustration of the configuration used in this example.

Figure 5-4 PAT with IPCP Single-Destination Negotiation



Cisco 765 Series Router Commands

Following are the commands for configuring the remote Cisco 765 series router for PAT with IPCP single-destination negotiation with a Cisco 4500 router:

```
set system 765
set ip pat po ftp 10.0.0.2
cd lan
set ip address 10.0.0.1
set ip netmask 255.0.0.0
set ip routing on
set user 4500
set active
set 1 number phone_number
set 2 number phone_number
set ip routing on
set ip rip version 2
set ip rip receive v2
set ip pat on
reboot
```

For detailed information regarding the commands listed here, refer to the *Cisco 700 Series Router Command Reference.*

Verify the Configuration

When a demand call is made, you can use the **show ip config all** and **show ip route all** commands to see the IPCP negotiation address.

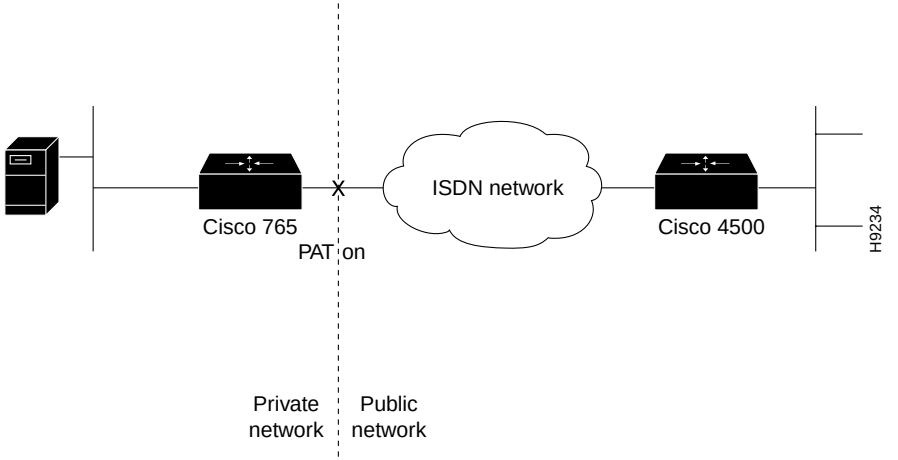
You can use the **show ip pat** command to see the services returned by PAT.

DHCP Server and PAT with IPCP Single-Destination Negotiation Example

This section describes how to configure a remote Cisco 700 series router for DHCP server with PAT and IPCP single-destination negotiation to a Cisco 4500 series router running Cisco IOS software at a central site.

Figure 5-5 is an illustration of the configuration used in this example.

Figure 5-5 DHCP Server with PAT and IPCP Single-Destination Negotiation



Cisco 765 Series Router Commands

Following are the commands for configuring the remote Cisco 765 series router for PAT with IPCP single-destination negotiation with a Cisco 4500 router:

```
set system 765
set ppp secret client
set ppp password client
set dhcp server
set dhcp address 172.168.99.2 128
set dhcp netmask 255.255.255.0
set dhcp gateway primary 172.168.99.1
set ip pat porthandler ftp 172.168.99.3
cd lan
set ip routing on
set ip address 172.168.99.1
set ip netmask 255.255.255.0
set user 4500
set 1 number phone_number
set 2 number phone_number
set ip routing on
set ip route destination 0.0.0.0/0 gateway 0.0.0.0
set ip address 0.0.0.0
set ip netmask 0.0.0.0
set ip pat on
set active
```

For detailed information regarding the commands listed here, refer to the *Cisco 700 Series Router Command Reference*.

Verify the Configuration

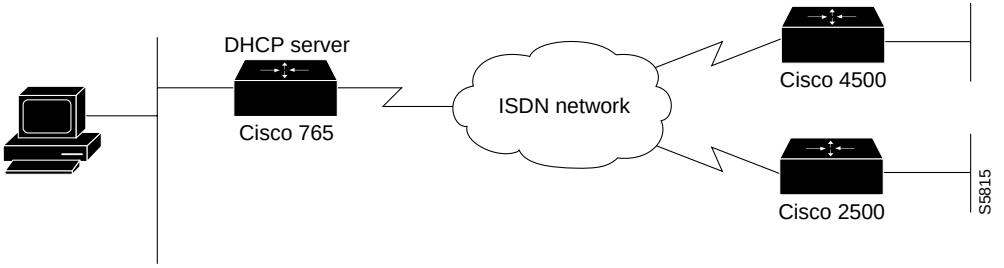
When a demand call is made, you can use the **show ip config all** and **show ip route all** commands to see the IPCP negotiation address. You can also use the **show dhcp config** and **show ip pat** commands to verify the configuration.

DHCP Server with PAT and IPCP Dual-Destination PPP Negotiation Example

This section describes how to configure a remote Cisco 700 series router for DHCP server with PAT and IPCP dual-destination PPP negotiation to two routers running Cisco IOS software.

Figure 5-6 is an illustration of the configuration used in this example.

Figure 5-6 DHCP Server with PAT and IPCP and Dual-Destination PPP Negotiation



Cisco 765 Series Router Commands

Following are the commands for configuring the remote Cisco 765 series router as a DHCP server with PAT and IPCP multilink PPP to two routers running Cisco IOS software:

```
set system 765
set ppp secret client
set ppp password client
set dhcp server
set dhcp address 172.168.99.2 128
set dhcp netmask 255.255.255.0
set dhcp gateway primary 172.168.99.1
set ip pat porthandler ftp 172.168.99.3
cd lan
set ip routing on
set ip address 172.168.99.1
set ip netmask 255.255.255.0
set user 2500
set ppp clientname 2500
set 1 number phone_number
set 2 number phone_number
set ip routing on
set ip route destination 0.0.0.0/0 gateway 30.169.100.2
set ip address 30.169.100.1
set ip netmask 255.255.255.0
set ip pat on
set active
set user 4500
set ppp clientname 4500
set 1 number phone_number
set 2 number phone_number
set ip routing on
set ip route destination 120.50.40.0/0 gateway 173.100.10.2
set ip address 173.100.10.1
set ip netmask 255.255.255.0
set ip pat on
set active
```

Note If you create a multiple destination configuration with PAT enabled in both profiles, the IP route destination must be specified, using the **set ip route destination** command.

Verify the Configuration

When a demand call is made, you can use the **show ip configuration all** command to see the IPCP negotiation address.

You can use the **show dhcp connections** command to see the IP addresses returned by DHCP.

CHAPTER 6

Configuring Remote CAPI

This chapter provides procedures for configuring Remote Common Application Programming Interface (CAPI) support on a Cisco 700 series router.

CAPI is an application programming interface standard used to access ISDN equipment connected to Basic Rate Interfaces (BRIs) and Primary Rate Interfaces (PRIs). CAPI provides a standardized interface that allows application programs to use ISDN drivers and controllers. One application can use one or more controllers. Several applications can share one or more controllers.

CAPI provides a selection mechanism that supports applications that use different protocols at different protocol levels. CAPI also provides standardized network access by performing an abstraction from different protocol variables. All connection-related data, such as connection state, display messages, and so on, is available to the applications at any time.

The framing protocols supported by CAPI consist of High-Level Data Link Control (HDLC), HDLC inverted, bit-transparent (speech), and V.110 synchronous/asynchronous.

CAPI integrates the following data link and network layer protocols:

- Link Access Procedure on the D channel (LAPD) in accordance with Q.921 for X.25 D-channel implementation
- Point-to-Point Protocol (PPP)
- ISO 8208 (X.25 DTE-DTE)
- X.25 DCE, T.90NL, and T.30 (fax group 3)

CAPI and RVS-COM

The Cisco 700 series router supports the ISDN Device Control Protocol (ISDN-DCP) from RVS-COM. ISDN-DCP allows a workstation on the LAN to use legacy dial computer telephony integration (CTI) applications. These applications include fax transmitting and receiving and placing and receiving phone calls.

Using ISDN-DCP, the router acts as a DCP server. By default, the router listens for DCP messages on TCP port number 2578 (the Internet-assigned number for RVS-COM DCP) on its LAN port.

When the router receives a DCP message from a DCP client (connected to the LAN port of the router), the router processes the message and acts on it. The actions consist of sending confirmations to the DCP clients and sending ISDN packets through the router BRI port.

When the router receives a packet on its BRI port for one of the DCP clients, the router formats the packet as a DCP message and sends it to the corresponding client. The router supports all the DCP messages specified in the ISDN-DCP specification.

The router provides two 64-kbps B channels to CAPI clients. Each B channel can be configured separately to work in either HDLC mode or bit-transparent mode. For CAPI support, the higher layer protocols (B2 through B7) are transparent to the applications using these B channels.

The ISDN Core Engine of RVS-COM supports the following B channel protocols:

- CAPI layer B1
  - 64 kbps with HDLC framing
  - 64-kbps bit-transparent operation with byte framing from the network
  - T.30 modem for fax group 3
  - Modem with full negotiation
- CAPI layer B2
  - X.75 SLP (ISO 7776) with V.42bis compression option (negotiated)
  - V.120 with V.42bis compression option (negotiated)
  - Transparent
  - T.30 modem for fax group 3

  - Modem with full negotiation
- CAPI layer B3
  - Transparent
  - T.90NL with compatibility with T.70NL, according to T.90 Appendix II
  - ISO 8208 (X.25 DTE-DTE) modulo 8 and windows size 2, no multiple logical connections
  - T.30 for fax group 3
  - Modem with full negotiation
- T.30 for fax group 3 (SFF file format [default], sending and receiving up to 14400 bps with ECM option, modulations V.17, V.21, V.27ter, V.29)
- Analog modem (sending and receiving up to 14400 bps with V.42 error correction and V.42bis compression option, modulations V.21, V.22, V.22bis, V.23, V.32, V.32bis)

Supported D-Channel Protocols

CAPI support is available only for the ISDN switch type Net3.

Supported Applications

ISDN-DCP supports CAPI and non-CAPI applications. Supported applications consist of those that use one or two B channels for data transfer, different HDLC-based protocols, Euro File transfer, or fax G4; also supported are applications that send bit-transparent data, such as A/Mu lay audio, fax G3, analog modem, or analog telephones.

Remote CAPI Router Commands

The commands used in this chapter have been added to the router user interface to support CAPI. Note that CAPI runs on a remote network device, not the router; the Cisco 700 series router enables remote CAPI applications.

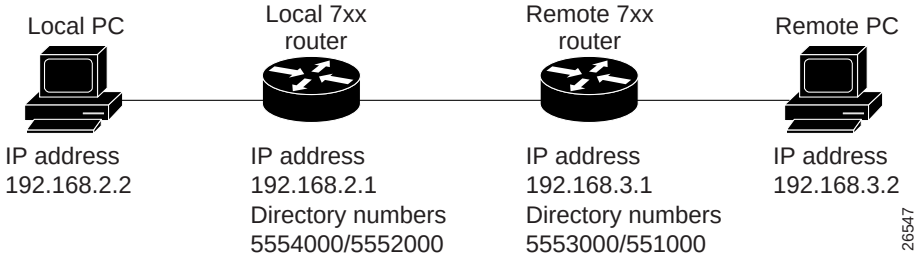
Configuring the Cisco 700 Router as an RCAPI Server

This section describes how to configure the Cisco 700 series router to be an RCAPI server.

By default, RCAPI is disabled in the router. Enabling RCAPI causes the router to become an RCAPI server. When RCAPI is enabled, the router listens for incoming RCAPI messages from PCs connected on its LAN side. By default, the router listens for RCAPI messages on TCP port 2578.

Figure 6-1 illustrates the configuration used in this example. The PCs in the figure have RVS-COM software installed.

Figure 6-1 RCAPI Server Configuration Example



RCAPI Command Summary

Following is the command summary for configuring the RCAPI on the local Cisco 700 series router.

```
set rcapi on
set dir 5554000
set rcapi 1 number 5554000
set rcapi server port 2578
reboot
```

Verify the Configuration

You can use the command **show rcapi status** to see the status of RCAPI server, the clients that are in the listening state, and the status of RCAPI calls:

```
local-router> show rcapi status
Rcapi Sever ON
Rcapi Server Port 2578
Rcapi Number(s) 5554000

CLIENT        SESSION-ID LISTEN CONNECTION-ID TYPE           CALL-STATUS
------------------------------------------------------------------------
192.168.100.3 16777218   ON
```

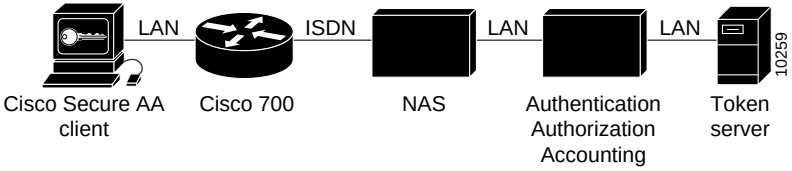
Token Card and Cisco Secure Authentication Support

This appendix provides Token Card and Cisco Secure Authentication support concepts as they apply to the Cisco 700 series router. Cisco Secure Authentication Agent supports *single-user mode*, which extends B channel authentication to a Cisco Secure Authentication Agent client.

Token cards are considered the most secure authentication solution available. There are two kinds of token cards, synchronous and asynchronous. Currently, Cisco Secure Authentication Agent only supports synchronous token card, which does not need a challenge from a token server to generate a token.

Figure A-1 shows the connection between the client and the token server.

Figure A-1 Cisco Secure Authentication Agent Client-to-Token Server Connection



The following steps illustrate how a link is established using a profile:

Step 1 Demand traffic or a **call** command makes a connection.

Step 2 The router sends a User Datagram Protocol (UDP) packet to a Token Authorization agent (also known as Cisco Secure Authentication Agent), requesting a username and password for PAP and CHAP. If Token Authorization Support (TAS**)** is set to **central**, the router always sends the authentication information request to the designated client.

Otherwise, the router sends the request to the source of the interesting packet received if the interesting packet is an IP packet. The router sends the request to the designated client if the interesting packet is not an IP packet.

Step 3 The agent software recognizes the UDP/IP packet and opens an authentication window on the terminal. The user enters the username and token. The agent organizes the information into the PAP and CHAP username and password, based on the router configuration. It then sends the username and password back to the router as a reply packet.

Step 4 The reply packet is received, and the router opens an ISDN connection with Network Access Server (NAS).

Step 5 The router negotiates all line-control protocol options, including which authentication protocol to use (PAP or CHAP).

Step 6 Depending on which authentication protocol is negotiated, the router assembles a PAP request or CHAP response packet and sends it to NAS. If authentication fails, NAS passes the failure message from authentication, authorization, and accounting (AAA) to the router. The router sends one more request to the agent with a message to retry once more. If authentication fails again, the router sends another PAP request with the **pppautheninfotype** parameter set to **message-only** to inform the Cisco Secure Authentication Agent client that the authentication failed again and that the router has stopped authorization attempts.

Token Caching

Cisco 700 series routers do not do token caching. A token is cached at the client, and the client sends the router the cached token in response to the authentication request from a link that uses a multilink PPP bundle. With its built-in algorithm, the agent can also generate a new token, called a *soft token*, instead of prompting the user to enter a new *hard token*.

There are two authentication modes, PAP and CHAP local secret, shown in the following figures.

Figure A-2 PAP Client Packet

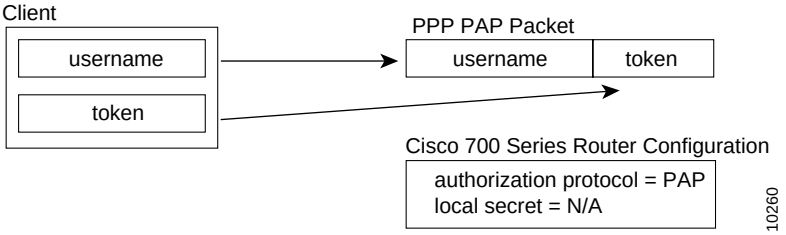
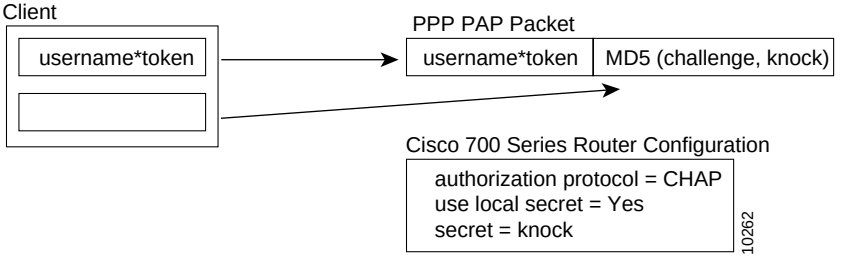


Figure A-3 CHAP Local Secret



Numerics

5ESS 3-6

A

Address Resolution Protocol
  See ARP
address, MAC 3-8
addressing, DHCP 5-2
AppleTalk 4-15
ARP, supported protocol 1-1
authentication 2-4
  CHAP 3-4
  PPP 3-8
autodetection
  set autodetection command 3-5
  troubleshooting 3-6

B

B channel 3-6
BCP, supported protocol 1-1
Bridge Control Protocol
  See BCP
bridging 3-7, 4-15
  configuration example 3-7
  interoperability issues 4-15

C

CAPI 6-1
caution description x
cd command 2-5
Challenge Handshake Authentication Protocol
  See CHAP
changing a profile name 2-6
CHAP 3-10
  authentication 3-10
  configuration example
    IP static routing and callback 4-2
    IP static routing with MLP 4-4
    IP unnumbered routing with MLP 4-8
    with Cisco IOS software 4-2, 4-4, 4-8
  secret 3-4
  supported protocol 1-2
Cisco Fast Step 1-3
Cisco Internetwork Operating System
  See Cisco IOS
Cisco IOS
  configuration vii, 4-1
  Release 11.0(3) 4-14
  Release 11.1 4-15
  software, interoperability with IPCP and IPXCP 5-4
  with bridging 4-15
Cisco IOS-700 software 1-2
command reference viii
Common Application Programming Interface
  See CAPI
  See Remote CAPI
configuration
  bridging example 3-7
  changing profiles 2-2
  displaying profiles 2-5
  example
    bridging 3-7
    IP static and callback with CHAP 4-2
    IP static with CHAP and MLP 4-4
    IP static with PAP 4-6
    IP unnumbered and CHAP with MLP 4-8
    RCAPI 6-4
    routing a Cisco 700 series router 3-9
    routing IP and IPX on-demand 3-14

routing to an ISP 3-9
ISDN PRI 4-1
line 3-5
options 1-3
port 1-3
profiles 2-1
Remote CAPI example 6-4
system level 2-2
Telnet 1-3
Web sources viii
connections
ISP 3-9
creating profiles 2-5

D

deleting profiles 2-6
demand RIP 4-14
DHCP
clients 5-2
default gateway 5-2
network addresses 5-2
relay 5-1
with IPCP negotiation 5-6
server 5-2
with IPCP negotiation 5-7
with PAT and IPCP dual-destination PPP negotiation 5-13
with PAT and IPCP single-destination negotiation 5-11
supported protocol 1-2
DMS-100 ISDN BRI switch 3-7
document conventions ix
documentation viii
documentation CD-ROM viii
Dynamic Host Configuration Protocol
See DHCP

F

firewall 5-3

I

ICMP, supported protocol 1-1
image (software) 1-3
Integrated Services Digital Network
See ISDN
Internal profile 2-4, 5-3
Internet Control Message Protocol
See ICMP
Internet Packet Exchange Control Protocol
See IPXCP
Internet Protocol Control Protocol
See IPCP
Internet service provider
See ISP
Internetwork Packet Exchange
See IPX
interoperability with Cisco IOS software
bridging 4-15
IPCP and IPXCP 5-4
multilink PPP encapsulation 4-14
IP 3-14, 3-17
configuration example
IP static and callback with CHAP 4-2
IP static with CHAP and MLP 4-4
IP static with PAP 4-6
IP unnumbered and CHAP with MLP 4-8
routing IP and IPX on-demand 3-14
DHCP
network addresses 5-2
relaying configuration information 5-1
unnumbered IP address 3-9
IPCP
interoperability 5-1
supported protocol 1-1

IPX 3-14, 3-17
  configuration example, routing IP and IPX on-demand 3-14
IPXCP
  interoperability issues 5-1
  supported protocol 1-1
ISDN
  BRI number 3-6
  PRI configuration 4-1
ISDN Device Control Protocol
  See ISDN-DCP
ISDN-DCP, supported protocol 1-2
ISP, connections 3-9

L

LAN
  Ethernet 10BaseT connection 3-2
  profile 2-4
LCP 3-11
line configuration 3-5
Link Control Protocol
  See LCP

M

MAC address table 3-8
MLP, configuration example
  IP static routing with CHAP 4-4
  IP unnumbered routing with CHAP 4-8
MLPPP
  encapsulation 4-14
  supported protocol 1-1
Multilink Point-to-Point Protocol
  See MLPPP

N

NCP 3-11
NetBIOS 4-15
network address
  DHCP 5-2
  space limitations 4-15
Network Control Protocol
  See NCP
NI1 switch 3-7
nonvolatile random access memory
  See NVRAM
note, description x
Novell IPX 4-15
NVRAM 2-1

O

operating system (router) 1-1
overview of Cisco 700 series routers 1-1

P

PAP 3-4
  configuration example
    IP static routing 4-6
    with a router running Cisco IOS software 4-6
  supported protocol 1-1
Password Authentication Protocol
  See PAP
PAT with IPCP single-destination negotiation 5-9
PAT, supported protocol 1-2
permanent profiles 2-4, 2-6
Point-to-Point Protocol
  See PPP
Port Address Translation
  See PAT

PPP 3-11
configuration example
routing IP and IPX on-demand 3-14
IP and IPX routing 3-14
IPCP negotiation 5-5
multilink encapsulation, interoperability 4-14
supported protocol 1-1
private IP addresses 5-3
profile-level parameters 2-1
profiles
active 2-2, 2-6
changing a profile name 2-6
creating 2-5
definition 3-2
deleting 2-6
displaying configurations 2-5
inactive 2-2, 2-6
on-demand 2-2
parameters 2-2
permanent 2-4
Internal 2-4
LAN 2-4
Standard 2-4
redefined values indicator 2-5
removing parameters 2-5
system mode parameters 2-3
user-defined 3-10
using with the routers 2-1 to 2-7
protocols supported 1-1

Q

quick reference viii

R

release notes for Cisco IOS 700 software viii
Remote CAPI 6-3
configuration 6-4
configuration example 6-4
TCP port 6-4
Remote CAPI, supported protocol 1-2
Remote Common Application Programmers Interface
See RCAPI
removing profile parameters 2-5
reset user command 2-6
RIP
dynamic routing protocols 4-14
PAT enabled 5-3
supported protocol
router manuals viii
routing
configuration example
bridging 3-7
central site 3-11
routing a Cisco 700 series router 3-9
routing IP and IPX on-demand 3-14
routing to an ISP 3-9
Routing Information Protocol
See RIP

S

SAP, supported protocol 1-1
secret, CHAP 3-4
Service Advertisement Protocol
See SAP
set autodetection command 3-5
set default command 3-4
set ip framing command 5-4
set ip rip update command 4-14
set ppp multilink command 4-14
set profile user command 2-6
set switch command 3-6
set user command 2-3
show commands, defined 2-5
show configuration command 3-3

show dhcp configuration 5-7
show dhcp connections 5-15
show ip configuration command 5-6
show ip route command 5-6
show rcapi status command 6-5
Simple Network Management Protocol
  See SNMP commands
SNMP, supported protocol 1-2
software image 1-3
software, Cisco IOS-700 1-2
SPIDs 3-6
  autodetection 3-5
  definintion 3-5
  troubleshooting 3-6
supported protocols 1-1
  ARP 1-1
  BCP 1-1
  CHAP 1-2
  DHCP 1-2
  ICMP 1-1
  IPCP 1-1
  IPXCP
  ISDN-DCP 1-2
  MLPPP 1-1
  PAP 1-1
  PAT 1-2
  PPP 1-1
  RCAPI 1-2
  RIP
  SAP 1-1
  SNMP 1-2
  TFTP 1-2
system mode
  configuration parameters 2-2
  parameters 2-1

T

TFTP server 1-2
TFTP, supported protocol 1-2
timesaver, description x
Triggered RIP 1-2
Trivial File Transfer Protocol
  See TFTP

U

unnumbered IP address 3-9
unroutable protocols 4-15
unset command 2-5

W

WAN ISDN ports 3-2
World Wide Web viii